RSAC 2025 Conference

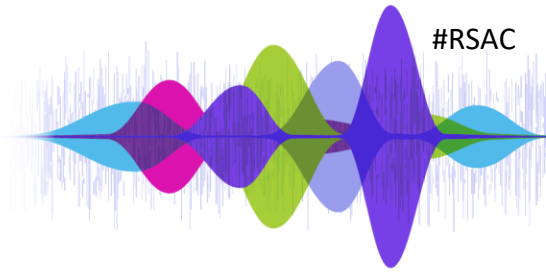
Many Voices.
One Community.

SESSION ID: IDY-T10

The Microsoft Cloud Identity Crisis

Guido Grillenmeier

Principal Technologist
Semperis
linkedin.com/in/guidogrillenmeier



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

WhoAMi

Guido Grillenmeier

Semperis Principal Technologist EMEA

1996 — HP invent

2003 – 2015 — Microsoft MVP Most Valuable Professional — *Category: Directory Services*

2015 — Hewlett Packard Enterprise

2018 — DXC.technology

2021 — semperis

RSAC 2025 Conference

What is a cloud identity crisis?

Imagine that an intruder breaches your Microsoft Entra tenant and hard deletes critical Entra ID objects …

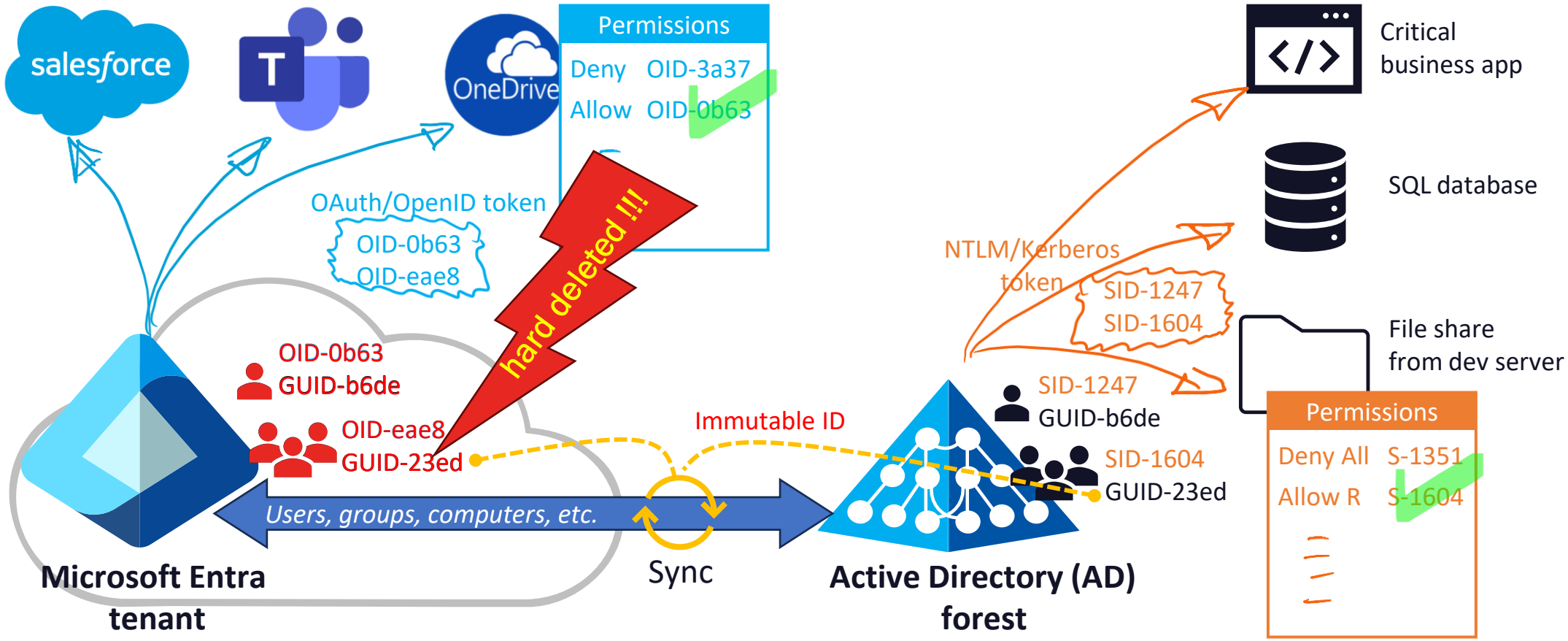
RSAC

W s?

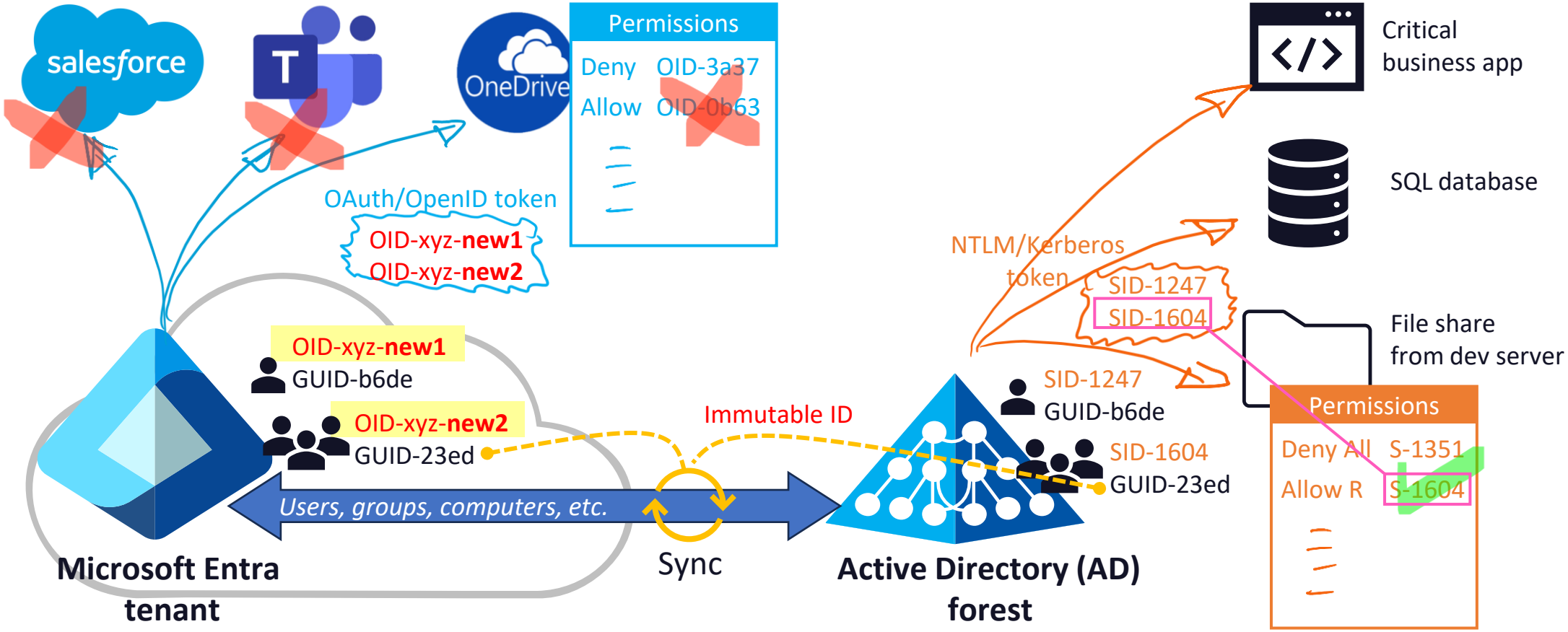
Imagin Entra
tena ...

What this would look like according to Copilot/Designer …

Microsoft hybrid identities rule the world



When cloud identities are hard deleted, things get ugly…



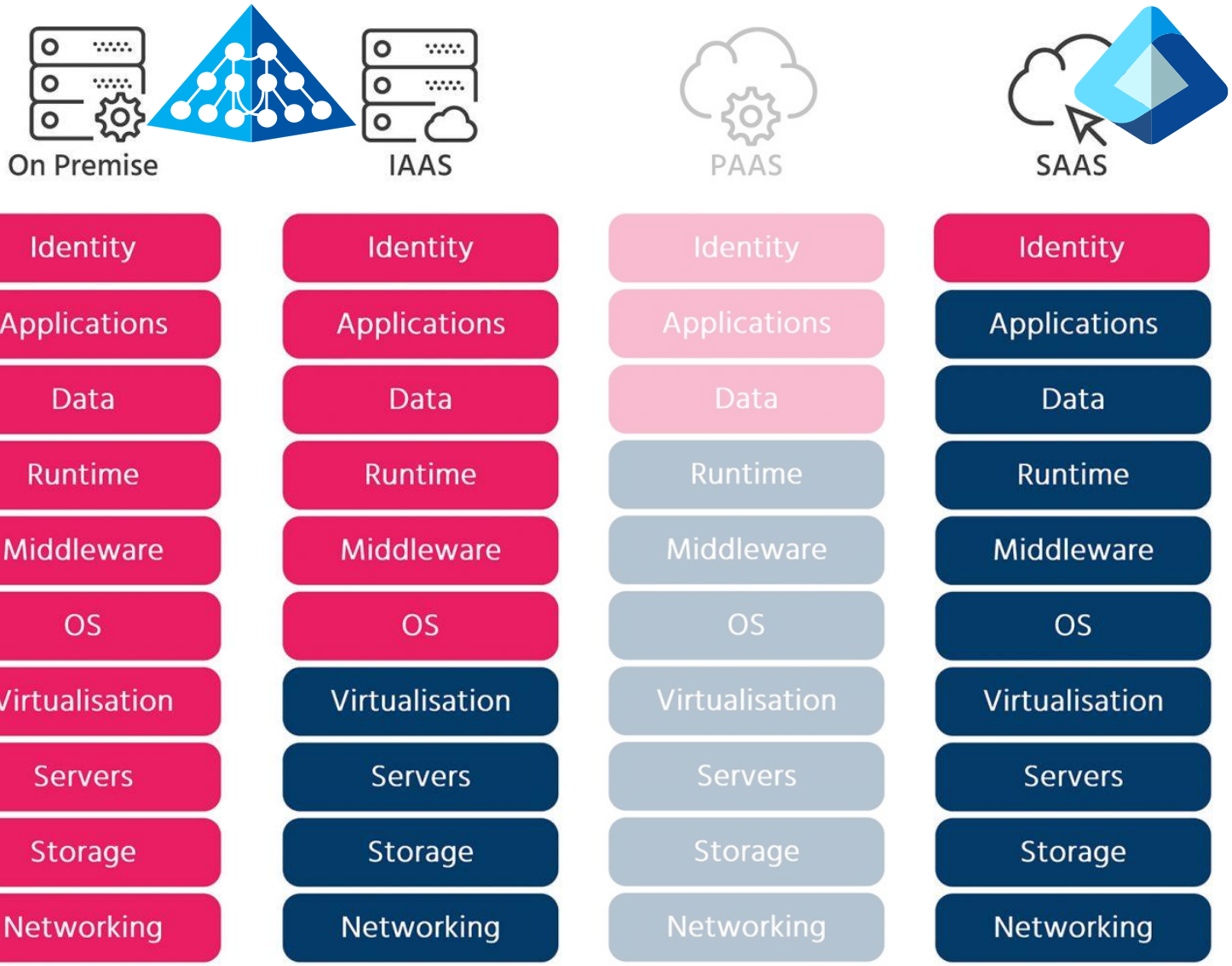
RSAC | 2025 Conference

Who is responsible for your cloud identities?

YOU are!

Many Voices.
One Community.

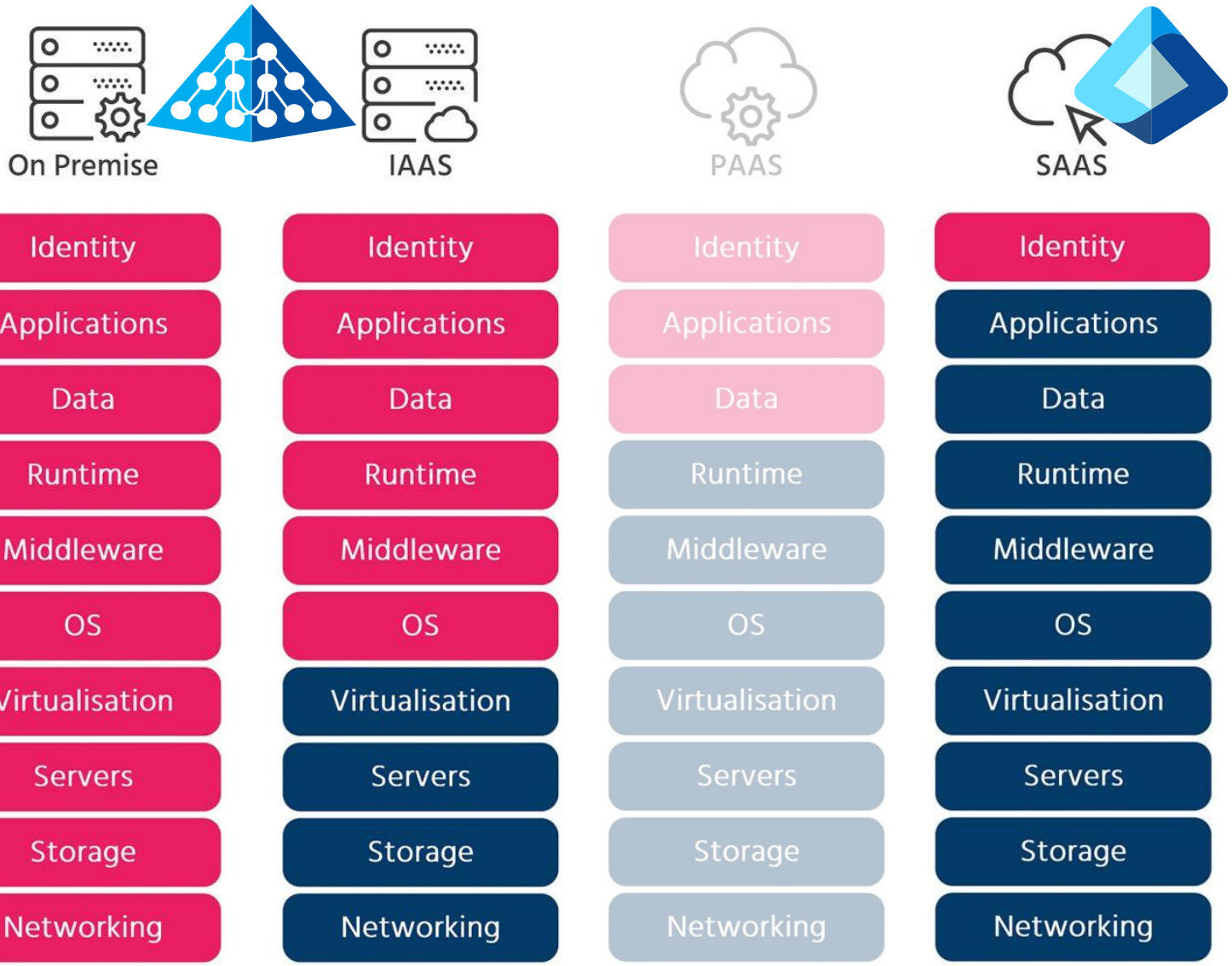
Shared responsibility model



You manage

Service provider manages

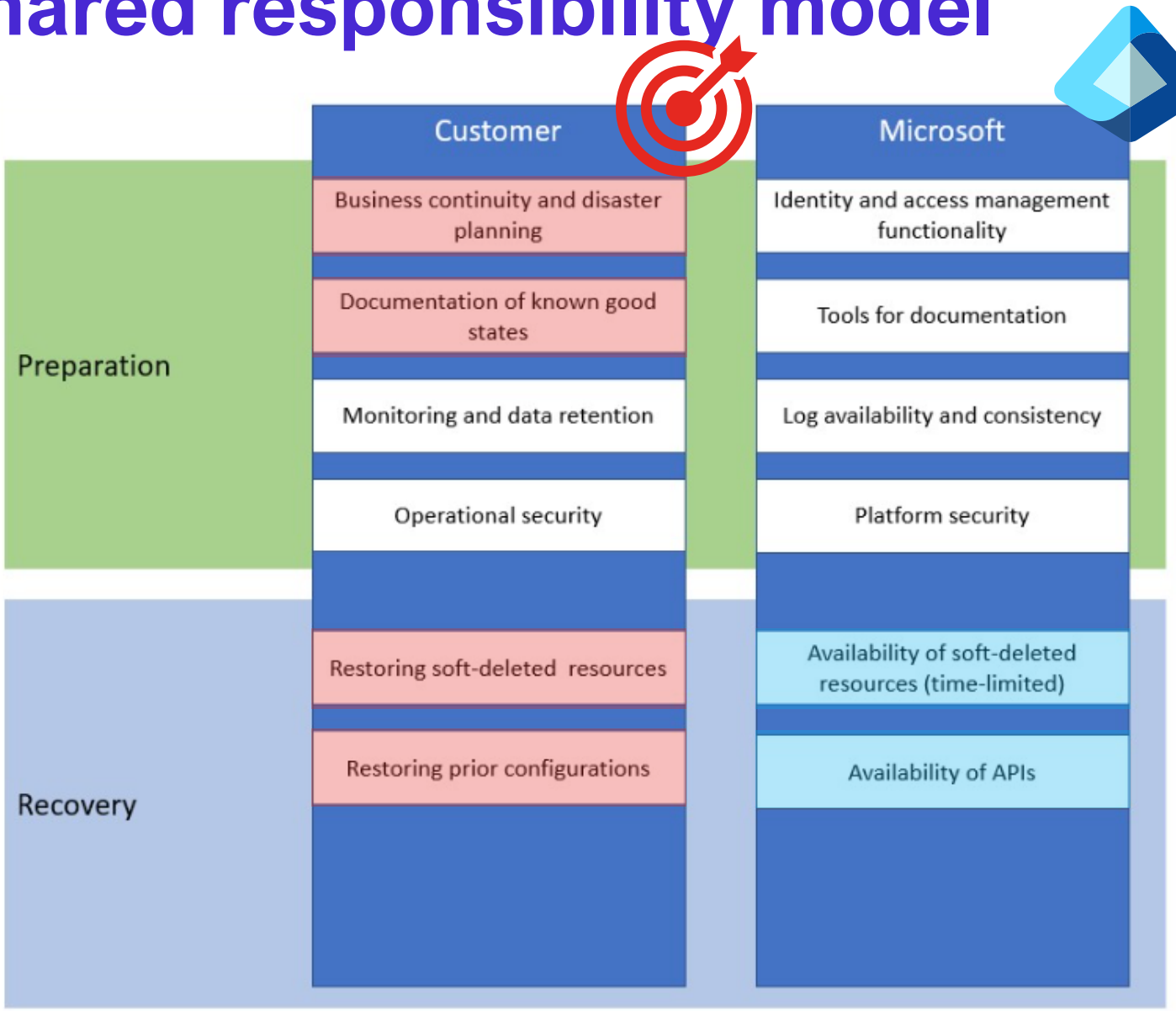
Shared responsibility model



You manage

Service provider manages

Shared responsibility model



Microsoft specifically calls out the **customer responsibility** for all aspects of **business continuity and disaster recovery** of Entra ID objects.

Microsoft's responsibility:

- **Soft delete feature**
- **APIs**

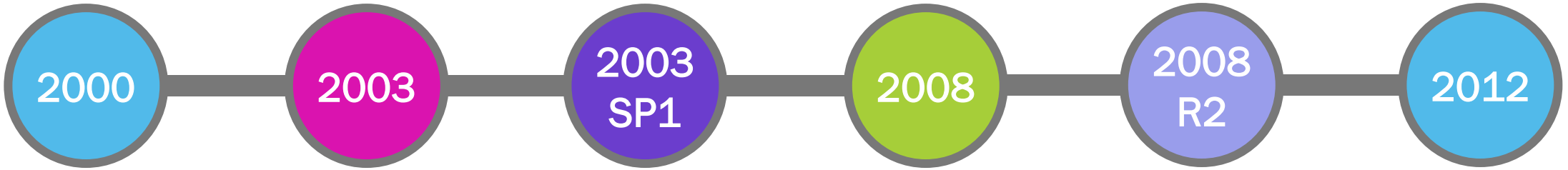
Source: https://learn.microsoft.com/en-us/entra/architecture/recoverability-overview

RSAC 2025 Conference

The key problem

Missing proper backup and recovery APIs for Entra ID objects

AD went through the same phases…



- Initial version of AD with Windows 2000 could not recover objects online.
- Tombstone reanimation was introduced with Windows Server 2003.
- Windows 2003 SP1 added SID History to the tombstone.
- Windows 2008 added new feature: Protect object from accidental deletion.
- Windows 2008 R2 gave us the Recycle Bin.
- Windows 2012 finally added a Recycle Bin UI.

Entra ID is still on a learning path

Plenty of objects, attributes, and configurations in Entra ID make out the overall service of one's own tenant.

Misconfigurations of various settings and policies—***possibly by malicious intent***—can affect security and user interactions and even cause denial of service.

Entra ID is still on a learning path

- https://learn.microsoft.com/en-us/entra/architecture/recover-from-deletions

Object type	Activity in log	Result
Application	Delete application	Soft deleted
Application	Hard delete application	Hard deleted
User	Delete user	Soft deleted
User	Hard delete user	Hard deleted
Microsoft 365 Group	Delete group	Soft deleted
Microsoft 365 Group	Hard delete group	Hard deleted
All other objects	Delete "objectType"	Hard deleted

Soft delete of **Devices** currently in preview!

ⓘ Note

The Audit log doesn't distinguish the group type of a deleted group. Only Microsoft 365 Groups are soft deleted. If you see a Delete group entry, it might be the soft delete of a Microsoft 365 Group or the hard delete of another type of group.

It's important that your documentation of your known good state includes the group type for each group in your organization. To learn more about documenting your known good state, see Recoverability best practices.

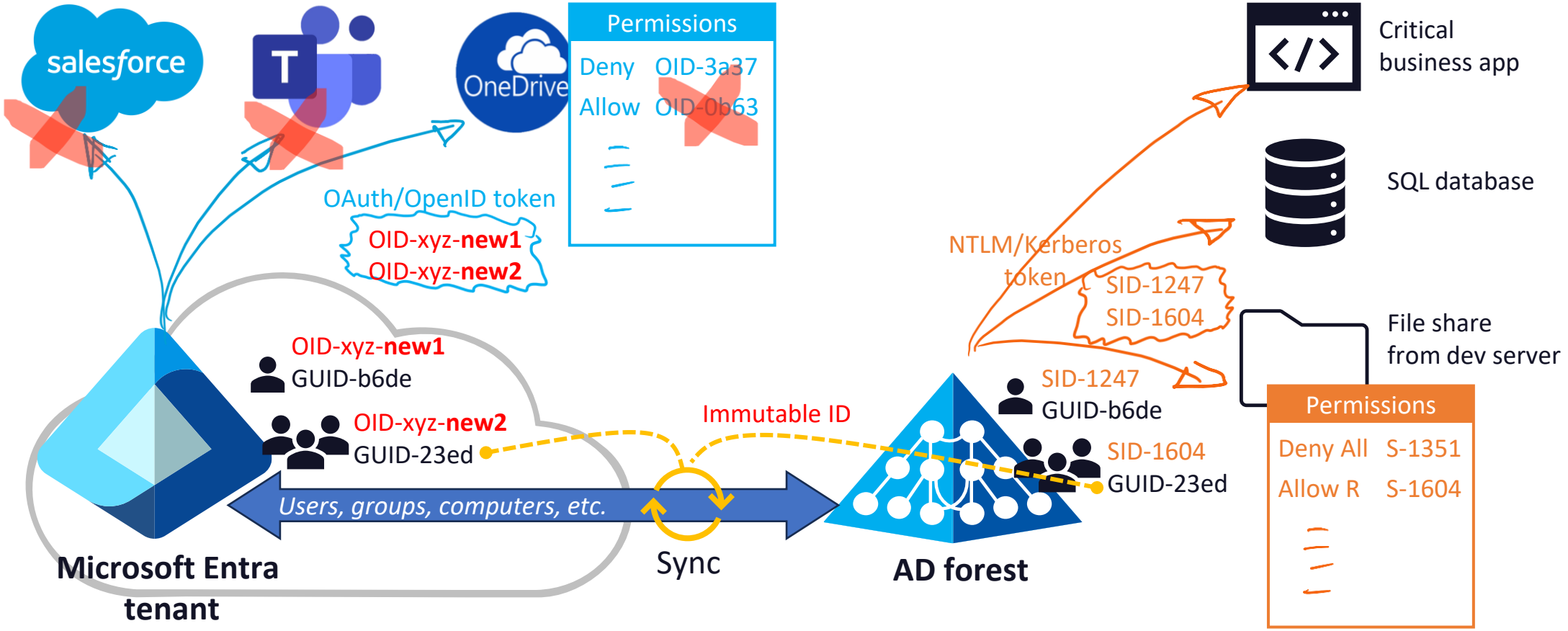
Entra ID is still on a learning path

- Soft delete is possible for only a few objects.
  - 30-day retention (*not configurable*)

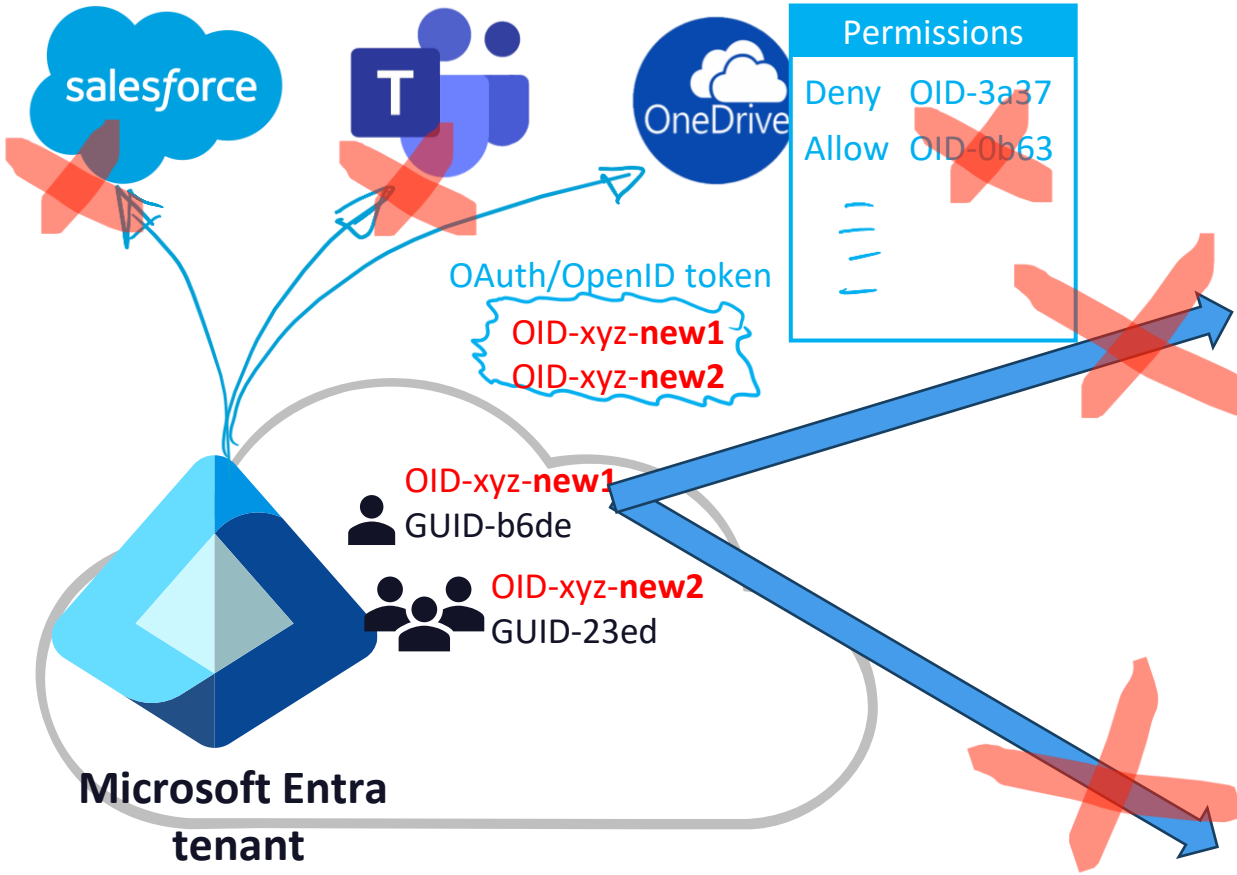
> ⓘ **Important**
>
> All other item types are hard deleted. When an item is hard deleted, it can't be restored. It must be re-created. Neither administrators nor Microsoft can restore hard-deleted items. Prepare for this situation by ensuring that you have processes and documentation to minimize potential disruption from a hard delete.

- Impactful Azure AD (now Entra ID) outage in 2020 ➔ addition of Azure AD authentication failover for FT in 2021.
  - Increased **authentication availability** from 99.9% to 99.99%
- Microsoft added purge protection for Azure storage blobs (*to protect against accidental or malicious hard deletes* of data), **but not for identity objects.**

When cloud identities are hard deleted, things get ugly…



When cloud identities are hard deleted, things get ugly…



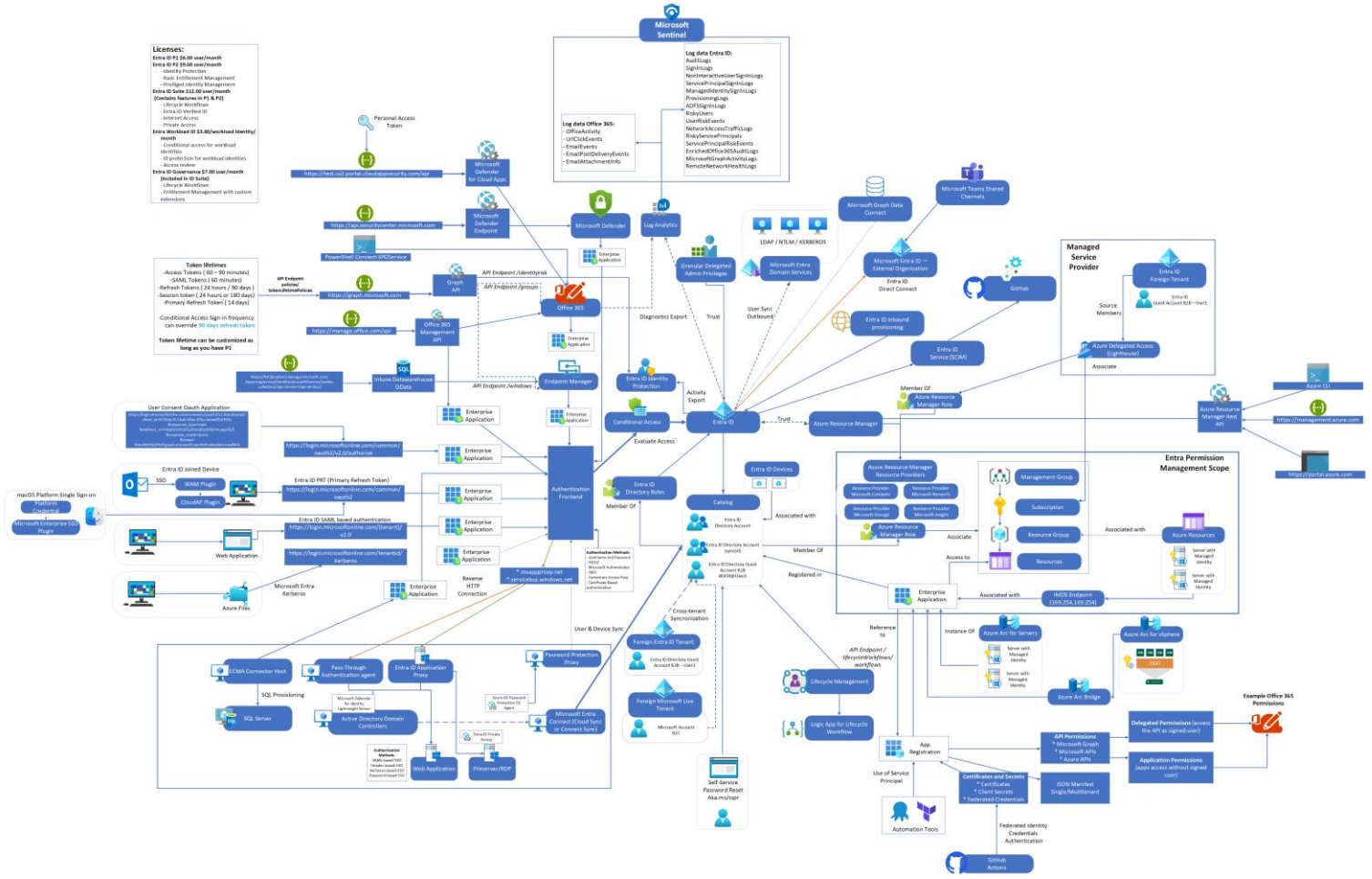
Various relationships within Entra tenant no longer work:

- Group memberships
- Role memberships
- Admin unit memberships
- Conditional access policies
- Applications
- Plus others

Non-accessible resources utilizing the Entra ID identity objects:

- All M365 apps (*email, SharePoint, Teams…*)
- Assigned Azure resources (*storage, VMs …*)
- Federated apps (*your business apps…*)
- Plus others

When cloud identities are hard deleted, things get ugly… and complicated!



https://github.com/msandbu/azuread/blob/main/EntraID-Overview.png

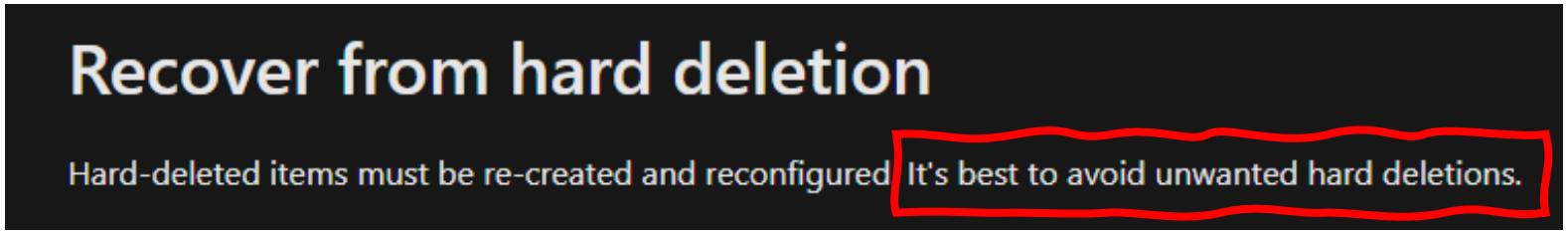
RSAC 2025 Conference

Reducing the risk

You must take various parallel approaches.

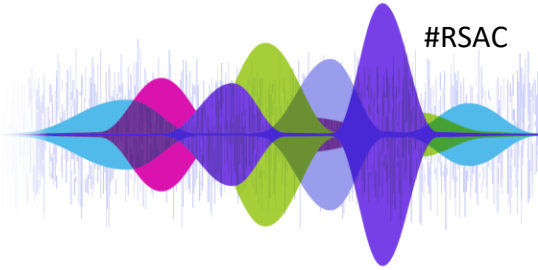
1: Prevent hard deletes

- Aligned with current Microsoft recommendation
  - https://learn.microsoft.com/en-us/entra/architecture/recover-from-deletions


Recover from hard deletion
Hard-deleted items must be re-created and reconfigured
It's best to avoid unwanted hard deletions.

- Use least-privilege approach
  - Easier said than done…given the extensive permissions on built-in roles
    - User Administrator ➔ *can manage **and delete** users **and groups***
    - Groups Administrator ➔ *can manage **and delete** groups (of any type)*
    - Cloud Device Administrator ➔ *can manage **and delete** devices*
    - Conditional Access Administrator ➔ *can manage **and delete** CAPs*
    - And so on

Refrain from using tenant scope roles



- Helps with protecting specific identity objects from “easy” hard deletion
- Make all unprivileged objects members of administrative units (AUs)
  - Relevant for users, groups, devices ➔ Assign roles to AU scope only
- Additional hurdle: restricted AUs
  - Even prevents (accidental) hard deletion by tenant scope roles (Global Admin, etc.)
  - Note: Global Admin can always grant themselves permissions to the AU…
- **Beware of limits**
  - AUs don’t protect from hard deletion of objects that do NOT have soft-delete status (e.g., “standard” Entra ID security groups)

More soft deletes required!

RSAC 2025 Conference

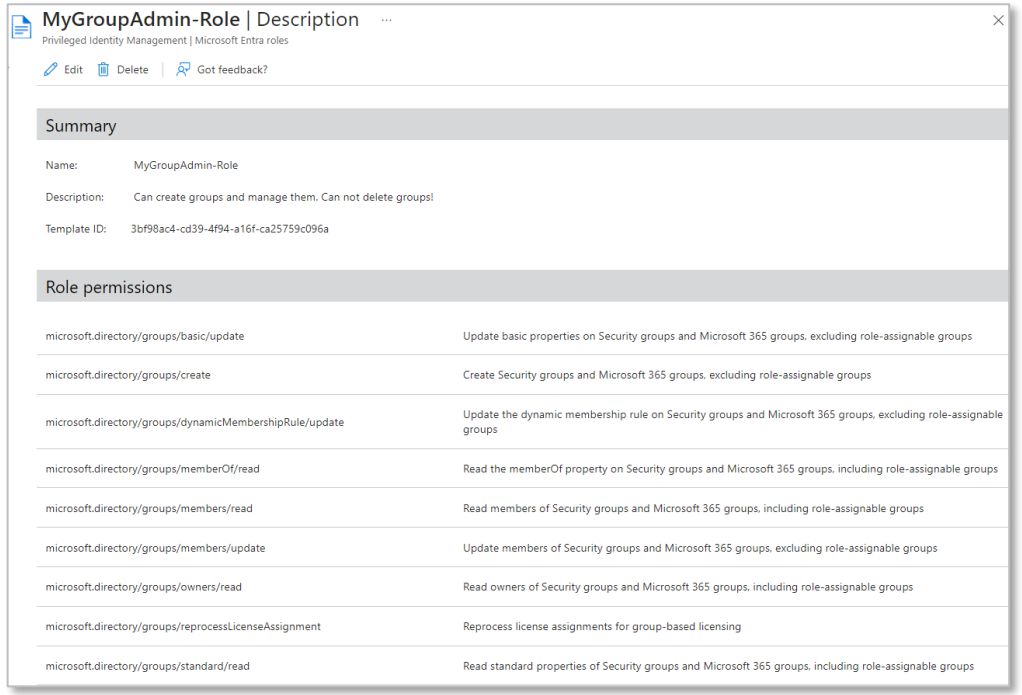
DEMO

Avoiding hard deletes

Many Voices.
One Community.

Better solution: custom roles

- Allows granting of specific change permissions only (*e.g., permissions to create and modify, but not delete, groups*)



MyGroupAdmin-Role | Description

Privileged Identity Management | Microsoft Entra roles

Edit | Delete | Got feedback?

Summary

Name:	MyGroupAdmin-Role
Description:	Can create groups and manage them. Can not delete groups!
Template ID:	3bf98ac4-cd39-4f94-a16f-ca25759c096a

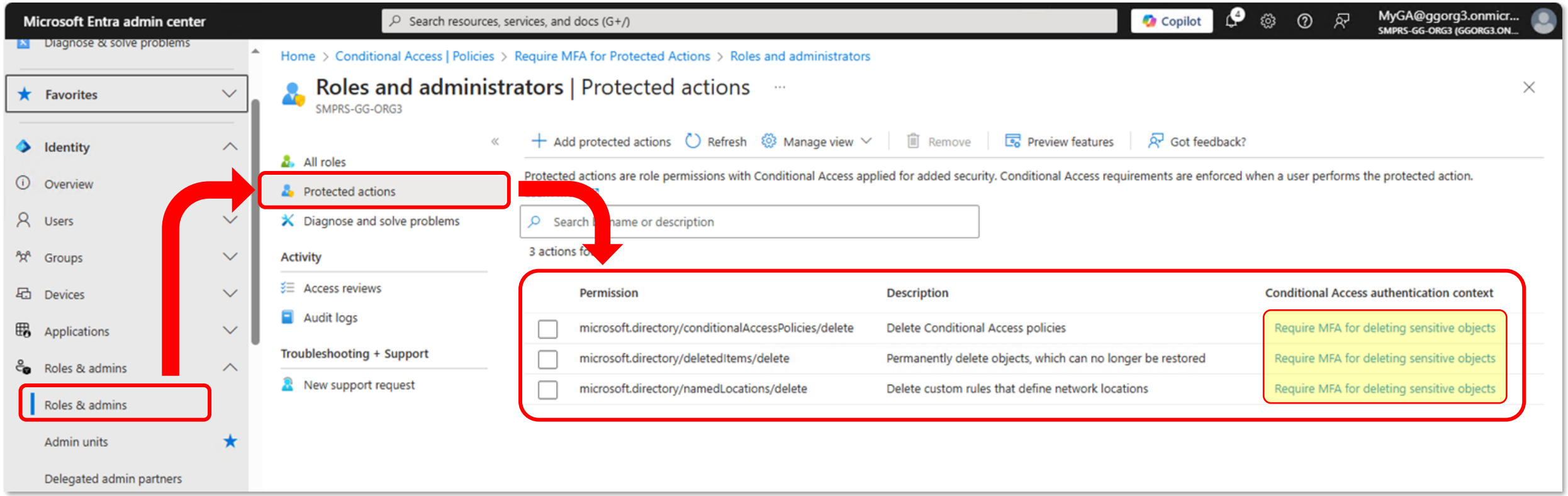
Role permissions

microsoft.directory/groups/basic/update	Update basic properties on Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/create	Create Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/dynamicMembershipRule/update	Update the dynamic membership rule on Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/memberOf/read	Read the memberOf property on Security groups and Microsoft 365 groups, including role-assignable groups
microsoft.directory/groups/members/read	Read members of Security groups and Microsoft 365 groups, including role-assignable groups
microsoft.directory/groups/members/update	Update members of Security groups and Microsoft 365 groups, excluding role-assignable groups
microsoft.directory/groups/owners/read	Read owners of Security groups and Microsoft 365 groups, including role-assignable groups
microsoft.directory/groups/reprocessLicenseAssignment	Reprocess license assignments for group-based licensing
microsoft.directory/groups/standard/read	Read standard properties of Security groups and Microsoft 365 groups, including role-assignable groups

- **KEY GOAL:** Treat **DELETES** of users, groups, devices, CAPs as a **PRIVILEGED task**

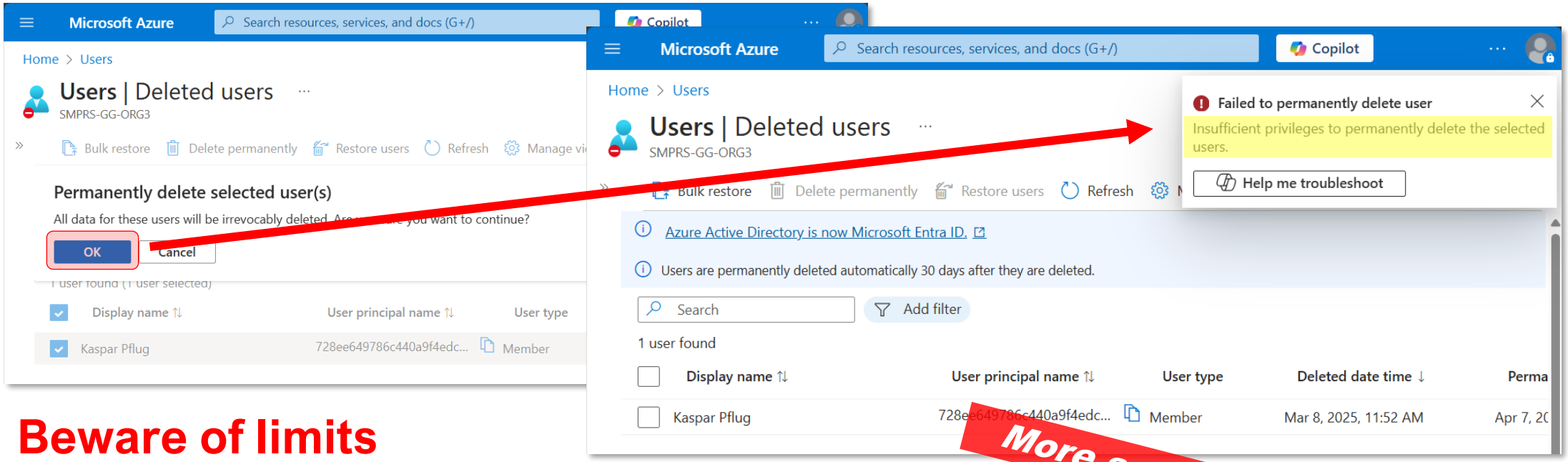
BRAND NEW (02/2025): Protected Actions
(for Deletion of Directory Objects)

- https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/protected-actions-overview#deletion-of-directory-objects
- Allows adding an **additional hurdle** before SOFT deleted objects can be HARD deleted (*applies to Users, M365 groups, and Apps*)



BRAND NEW (02/2025): Protected Actions
(for Deletion of Directory Objects)

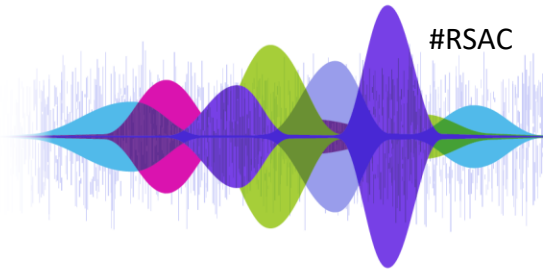
- https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/protected-actions-overview#deletion-of-directory-objects



- **Beware of limits**
  - Protected actions don't protect from hard deletion of objects that do NOT have soft-delete status (e.g., "standard" Entra ID security groups)

More soft deletes required!

2: Back up your Entra objects and relationships



- Can be done with scripts
  - Great PowerShell solution: **EntraExporter** from Merill Fernando (Microsoft)
    - https://github.com/microsoft/EntraExporter *(free)*
- Commercial solutions are also available
  - Some identity protection vendors offer fully automated backup **and recovery** of Entra objects and configuration.
- **BEWARE:** Regardless of the path you take, there is currently **no way** for you to export **secrets** or other sensitive attributes for any Entra ID objects.
  - User passwords
  - Certificates or ClientKeys for apps or SAML configuration
  - And so on

Missing APIs...

3: Test recovery

- Test recovery of dummy objects configured like a normal user
  - Improve understanding of the scope of the actual problem
  - Reconnect a hard deleted user to a mailbox after creating it
  - Learn how to recreate all those links to other Entra ID objects
- **Beware:** EntraExporter will only back up your data … *but not restore it*
  - Must take time to understand the data structure and how to use scripting to recreate objects
- Commercial solutions will do this for you
- **ADDITIONAL CHALLENGE:**
  Permissions on resources are typically set by **OID** of the Entra user or group …

Further recommendations

- Script/automate configuration settings in Entra ID and on cloud resources
  - Perfect documentation
  - Easily repeatable
- Beware of the risks using on-prem synchronized groups in Entra ID
  - Sync will automatically create “standard” Entra ID security groups
  - No soft-delete for this group-type ➔ a simple sync configuration mistake can wreak havoc
- Avoid assigning owners to “standard” security groups
  - Owners can delete the groups they own…
- Take the time to analyze the output of EntraExporter *(or other Entra ID exports)*
  - Get ready to recreate objects and their relationships
  - Save valuable time during a disaster

… or commercial solutions!

RSAC 2025 Conference

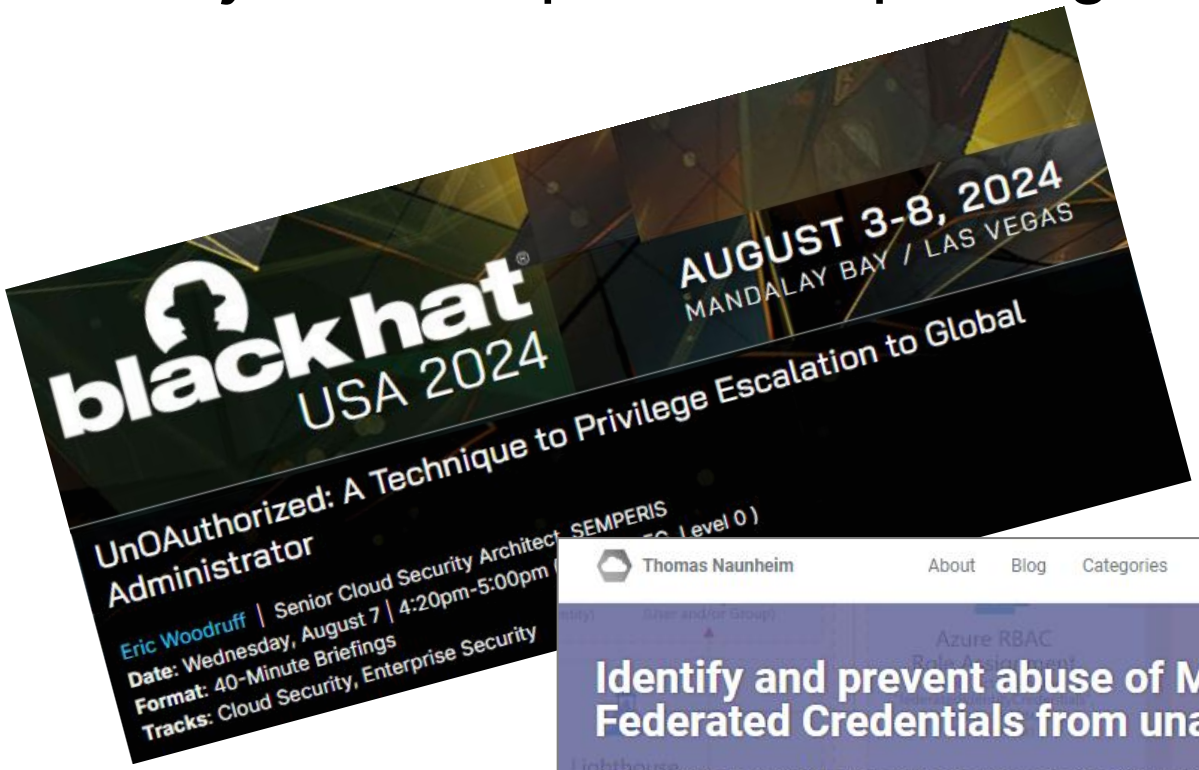
DEMO

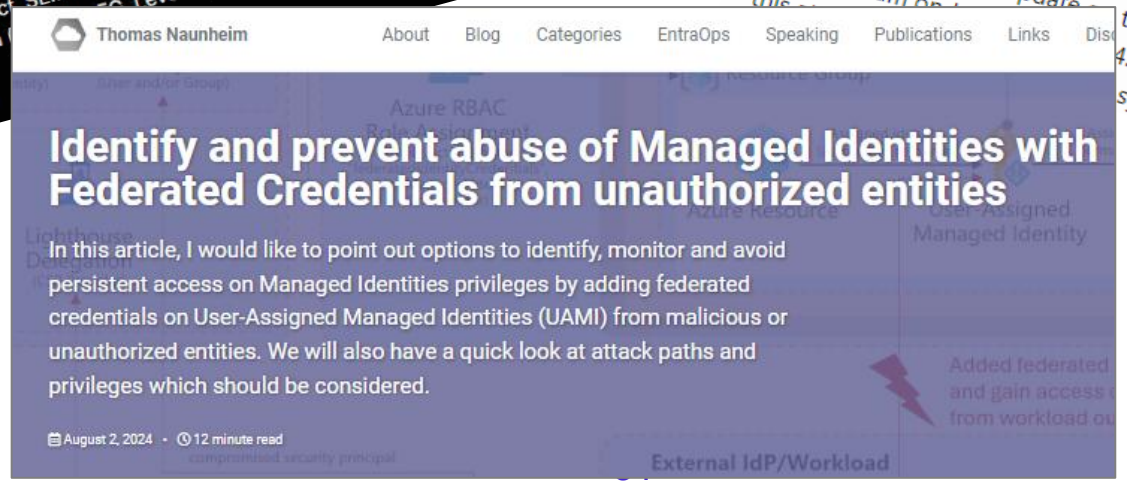
Using Output from EntraExporter to re-create deleted objects

Many Voices.
One Community.

Still a risky business…

…as you can't prevent a privileged user from hard-deleting objects


black hat
USA 2024
AUGUST 3-8, 2024
MANDALAY BAY / LAS VEGAS
UnOAuthorized: A Technique to Privilege Escalation to Global Administrator
Eric Woodruff | Senior Cloud Security Architect, SEMPERIS
Date: Wednesday, August 7 | 4:20pm-5:00pm
Format: 40-Minute Briefings
Tracks: Cloud Security, Enterprise Security


Thomas Naunheim
About
Blog
Categories
EntraOps
Speaking
Publications
Links
Identify and prevent abuse of Managed Identities with Federated Credentials from unauthorized entities
In this article, I would like to point out options to identify, monitor and avoid persistent access on Managed Identities privileges by adding federated credentials on User-Assigned Managed Identities (UAMI) from malicious or unauthorized entities. We will also have a quick look at attack paths and privileges which should be considered.
August 2, 2024 · 12 minute read

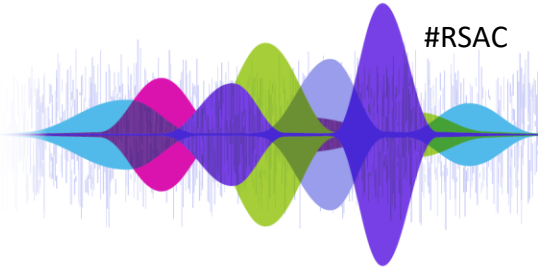
Need Purge Protection / Tenant Recovery
Microsoft
MSRC
Blog / 2024 / 03 / Update-On-Microsoft-Actions-Following-Attack-By-Nation-State-Actor-Midnight-Blizzard /
Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard
MSRC / By MSRC / March 08, 2024 / 2 min read
This blog provides an update
the nation-state attack that was detected by the Microsoft
4. As we shared, on January 19, the security team detected
systems and immediately activated our response process.

4: Raise your concerns to Microsoft

- As with any software vendor, Microsoft prioritizes features by customer demand
- Demand better identity protection, better backup/recovery APIs
- Talk to your TAM and demand a roadmap for identity backup and recovery
- Join the Microsoft Customer Connection Program (CCP): https://aka.ms/JoinCCP
  - Request to be registered as **Microsoft Entra Advisor**

13. Which Community Program are you interested in joining? *
Data Security and Privacy
Management (Windows, Microsoft Intune Suite, and Cloud PC)
Microsoft Entra Advisors
Security Connection Program (SIEM & XDR, Defender for Cloud, Network Security)
Copilot for Security

Avoid your own Cloud Identity Crisis!



- Next week you should:
  - Run a backup of all your Entra ID objects in your tenant
- In the first three months following this presentation you should:
  - Re-Evaluate your Entra ID role/delegation model
  - Test hard-deletion and recovery of well-defined dummy objects
- Within six months you should:
  - Automate your Entra ID backup & configuration to reduce risk
  - Perform an in-depth evaluation of the impact of mass hard-deletions of users & groups on your business
  - Talk to Microsoft and demand proper backup & recovery APIs

RSAC 2025 Conference

Many Voices.
One Community.

Thank You

For more information, see all links from talk on next slide.
And don't hesitate to reach out to me:

linkedin.com/in/guidogrillenmeier
GuidoG@semperis.com

Further resources *(Links and Tools)*

- **Entra ID recoverability:** https://learn.microsoft.com/en-us/entra/architecture/recoverability-overview
- **Recover from deletions:** https://learn.microsoft.com/en-us/entra/architecture/recover-from-deletions
- **Entra ID Backup Authentication Service:** https://azure.microsoft.com/en-us/blog/advancing-service-resilience-in-azure-active-directory-with-its-backup-authentication-service
- **Entra ID overview graphic:** https://github.com/msandbu/azuread/blob/main/EntraID-Overview.png
- **Protected Actions:** https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/protected-actions-overview#deletion-of-directory-objects
- **UnOauthorized:** https://www.blackhat.com/us-24/briefings/schedule/index.html#unoauthorized-a-technique-to-privilege-escalation-to-global-administrator-39231
- **Prevent abuse of federated credentials:** https://www.cloud-architekt.net/identify-prevent-abuse-uami-fedcreds/
- **Microsoft CCP:** https://aka.ms/JoinCCP
- **Privileged IAM in Entra ID:** https://github.com/Cloud-Architekt/AzurePrivilegedIAM
- **Free community tool – Purple Knight:** www.semperis.com/purple-knight
- **Free community tool – Forest Druid:** www.semperis.com/forest-druid